their view, the failure to fund the GIFC was proof of the State Department's diplomatic squeamishness about supporting a religious sect that the Chinese government considers a direct enemy.

Though the State Department did grant a small amount of funding to the GIFC in 2010, in January 2011 it announced that a remaining $28 million in unspent funds would support not only circumvention tools, but also technologies and organizations aimed at helping Internet users in repressive countries defend against a much broader range of threats, including total Internet shutdown (most famously deployed in Egypt but also used by other governments including Syria, Burma, and selectively by China in specific regions and locations); aggressive denial-of-service attacks on activist websites; spyware installed surreptitiously on activists' and journalists' computers; hacking of activists' social media accounts; and the deletion by Internet companies of sensitive content, deactivation of accounts, and tracking of user behavior.

In retaliation against the State Department for failing to support circumvention tools exclusively, Senator Richard Lugar, ranking Republican on the Senate Foreign Relations Committee, called for the remaining funds to be removed from State Department control and given to the Broadcasting Board of Governors (BBG), the government agency that runs the Voice of America, Radio Free Asia, Radio Free Europe and Radio Liberty, Al Hurra TV, and other US-government funded broadcasters. The BBG had been funding circumvention tools including the GIFC to help their audiences access their websites, and unlike the State Department, they committed to spend the funds exclusively on circumvention. In April 2011 after aggressive lobbying by GIFC supporters, Congress decided to split the difference, cutting the State Department's annual funding for Internet freedom technologies and training by one-third and giving that portion to the BBG, which was expected to continue funding the GIFC, among others.

In the end, roughly half of the State Department funding went to circumvention technologies, with the rest of the money spent on other projects, including mobile security technology and training on protecting against hacking and online surveillance, as well as a project that is

sometimes called "Internet-in-a-box" or "Internet-in-a-suitcase"—a set of tools and technologies for people to remain connected, at least in a rudimentary, ad hoc way, when networks get shut down.

Bizarrely, most of the people involved in the fight for Internet freedom funding said little and did nothing about a blatant contradiction: although US taxpayer money is being spent to help activists get around censorship, much of the censorship in North Africa and the Middle East is being carried out largely with North American software—as the Open Net Initiative's report on the sale of North American censorship technologies to repressive regimes has documented. This technology is "dual use" in the sense that it can also be used by families to protect children from inappropriate content or dangerous contact with ill-intentioned adults, or by network administrators to defend against attacks, but the extent to which companies are marketing their tools to repressive regimes—with full knowledge of how they will be used—has been the subject of much less energy and discussion in Washington than the issue of who ought to be receiving Internet freedom funds. Moreover, the fight over circumvention funding only further distracted politicians, policy makers, media pundits, and journalists from the deeper question of what Internet freedom actually means.

GOALS AND METHODS

Writing in *Foreign Affairs* in late 2010, New York University's Clay Shirky critiqued Washington's obsession with circumvention. Such an "instrumental" approach, he argued, is counterproductive in the long run. The main problem that circumvention technology aims to address is the blocking of content and platforms based *outside* a country, run by people over whom the government in question has no direct jurisdiction or control. Circumvention is much less helpful to people seeking to create their own content and build their own locally based information communities and networks. "The potential of social media," Shirky wrote, "lies mainly in their support of civil society and the public sphere—change measured in years and decades rather than weeks or

months." This was certainly the case for the Egyptian and Tunisian revolutions: journalists and policy researchers deconstructing events after the fact discovered that activists in these countries had spent years building not only an online community skilled in the use of social media, but also a network of offline ties and trusted relationships. Similarly, the efforts by beleaguered liberal Chinese bloggers and intellectuals, who struggled for nearly a decade to build and nurture both online and offline spaces for liberal-leaning, political criticism of the kind not permitted on Chinese commercial platforms, have been largely quashed by the Chinese government.

Concretely, if one applies Shirky's framework to the Chinese situation, one can see how the government's attack on a community of liberal-minded bloggers through arrest, threats, and harassment—a community with both online and offline components that took nearly a decade to build and deepen—is many magnitudes more insidious and harmful than the blockage of websites run by the Voice of America and Radio Free Asia, or even YouTube, Facebook, and Twitter. Instead of viewing the Internet and social media as instrumental to freedom, Shirky advocates what he calls an "environmental" approach, focused on the idea that "positive changes in the life of a country, including pro-democratic regime change, follow, rather than precede, the development of a strong public sphere." This requires a fundamental shift in strategy, from providing uncensored access to outside content to "securing the freedom of personal and social communication among a state's population, [which] should be the highest priority, closely followed by securing individual citizens' ability to speak in public. This reordering would reflect the reality that it is a strong civil society—one in which citizens have freedom of assembly—rather than access to Google or YouTube, that does the most to force governments to serve their citizens."

Others argue that the US government's Internet freedom policy should not treat the Internet as an instrument for regime change—especially given that some groups and governments elsewhere in the world are using the Internet to help weaken, challenge, or destabilize

the American system of government. Furthermore, as Ethan Zuckerman of Harvard's Berkman Center warns, if US policy approaches the Internet as if its main value is as a conduit for the Voice of America, repressive regimes will be more likely to treat American Internet companies—and the Western technology industry more generally—as enemy combatants. US-based Internet companies' local employees as well as their most active local users will more likely be viewed as foreign agents. Rather, Zuckerman argues, the goal should be much broader and ideologically agnostic: "to ensure that people can make their voices heard in this new space, and hope that governments will be wise enough to listen and to engage."

Writer and critic Evgeny Morozov has been even more critical of the US government's "Internet freedom" policy, warning that any policy based on the assumption that the Internet inherently helps democracy and hurts authoritarianism is misguided, counterproductive, and downright dangerous. His book *The Net Delusion* offers a scathing condemnation of the "cyber-utopian" and "Internet-centric" worldviews he believes to be epidemic among American academics (including Shirky and Zuckerman), alongside many activists, foundations, journalists, politicians, and investors. He mocks what he calls the "Google Doctrine—the enthusiastic belief in the liberating power of technology accompanied by the irresistible urge to enlist Silicon Valley start-ups in the global fight for freedom." Cyber-utopianism, he argues, is dangerous because it fails to recognize that the Internet "penetrates and reshapes all walks of political life, not just the ones conducive to democratization." The Internet, he points out, empowers dictators, demagogues, and terrorists as much as it empowers democrats. How the Internet interacts with politics and the particulars of how it is used for good and for ill vary drastically from country to country.

US Internet freedom policy also has critics among its intended beneficiaries overseas. Tunisian blogger and activist Sami Ben Gharbia—who was heavily involved in the movement to bring down the Ben Ali regime—wrote a passionate essay in September 2010, just four months before his government fell, explaining how US government involvement

in grassroots digital spaces can be counterproductive by endangering people who are already vulnerable to being accused by nasty regimes of being foreign agents and unhelpfully causing authoritarian governments to view Western Internet companies as their enemies. He quoted the Egyptian blogger and activist Alaa Abd El-Fattah, who argued that Western democracies must sort out their own domestic obstacles to Internet freedom if they want to be genuinely helpful to Middle Eastern Internet freedom and democracy in the long run:

> Fight the troubling trends emerging in your own backyards from threats to Net neutrality, disregard for user's privacy, draconian copyright and DRM [digital rights management] restrictions, to the troubling trends of censorship through courts in Europe, restrictions on anonymous access and rampant surveillance in the name of combating terrorism or protecting children or fighting hate speech or whatever. You see these trends give our own regimes great excuses for their own actions. You don't need special programs and projects to help free the Internet in the Middle East. Just keep it free, accessible and affordable on your side and we'll figure out how to use it, get around restrictions imposed by our governments and innovate and contribute to the network's growth.

Despite critiques from activists like Ben Gharbia and Abd El-Fattah and intellectuals like Morozov, and the challenges brought by WikiLeaks' release of confidential State Department cables at the end of 2010, Clinton was determined to press forward with her Internet freedom policy. In February 2011, at the height of the Arab Spring, she gave a second Internet freedom speech. Though events in the Middle East and North Africa seemed to have vindicated her department's belief in the Internet as a key policy priority, gone was the Churchillian tone and the Cold War metaphors of the previous year's speech. She admitted that neither she "nor the United States government has all the answers," or even all the right questions. Whether the

Internet—the "public space of the twenty-first century"—is used positively or negatively, she noted, depends on each and every one of the world's two billion–plus Internet users, as well as all governments who seek to regulate it, and companies that build Internet technologies and platforms.

Still, the State Department has been unable to escape the contradictions between US Internet freedom policies and Washington's pursuit of national security, counterterrorism, trade, and copyright interests. Many people around the world are cynical about these contradictions in precisely the same way that people are cynical about how US economic and security interests regularly contradict, and sometimes override, the degree to which the United States is willing to emphasize democracy and human rights in its diplomacy and assistance priorities with particular countries. Examples abound: In early 2011 protesters in several countries reported that, after being teargassed by riot police, they found empty gas canisters marked "made in USA" lying in the street. While the Bahraini government was arresting bloggers and suppressing dissent, the United States was planning to sell $70 million in arms to Bahrain. When Clinton visited Cairo a month after the revolution, Egypt's January 25 Revolution Youth Coalition refused to meet with her, because "the US administration took Egypt's revolution lightly and supported the old regime while Egyptian blood was being spilled."

Despite these hypocrisies and contradictions, the Obama administration is moving to reinforce, broaden, and institutionalize its Internet freedom policy, first championed by Clinton. In May 2011, the administration published a document called the "International Strategy for Cyberspace," outlining the US government's overarching goals in preserving the global Internet as an open, interoperable, secure, and stable network. "While offline challenges of crime and aggression have made their way into the digital world," wrote President Obama in the introduction, "we will confront them consistent with the principles we hold dear: free speech and association, privacy, and the free flow of information." The challenge now is for American citizens—and netizens everywhere—to hold the US government to this commitment. As Part

Three of this book discussed in detail, that will not be easy. Still, that the administration has made a free and open Internet into an official policy goal at least makes it difficult for US officials to ignore or discount public criticism of any US government actions that undermine Internet freedom.

DEMOCRATIC DISCORD

In the months following Clinton's first speech in January 2010, Internet freedom quickly became a buzzword in foreign ministries around the democratic world, especially in northern Europe. Swedish Foreign Minister Carl Bildt called for a "new transatlantic partnership for protecting and promoting the freedoms of cyberspace." His ministry then proceeded to take the lead in facilitating several international meetings over the ensuing year and a half, including two multi-stakeholder brainstorming conferences on global Internet freedom.

Positive momentum continued to build through the summer. In July 2010 the French and Dutch foreign ministers convened an international conference on the Internet and freedom of expression attended by representatives of seventeen governments, in addition to dozens of representatives from nongovernmental organizations, businesses, and international organizations. They announced agreement on several points, including that the international community must improve monitoring actions of governments to ensure that they protect—and avoid violating—online free expression; that there must be better mechanisms for holding companies accountable when they collaborate with repressive censorship and surveillance; and that more must be done to "come to the aid of cyber-dissidents." They also agreed to hold two more meetings later in the fall.

Unity crumbled before any further meetings could take place. Less than a month before the next conference, planned for Paris in late October, President Nicolas Sarkozy declared in a speech at the Vatican, "Regulating the Internet to correct the excesses and abuses that arise from the total absence of rules is a moral imperative." Soon thereafter,

the French free speech organization La Quadrature du Net published a leaked letter from Sarkozy to French Foreign Minister Bernard Kouchner, in which Sarkozy described the conference as an "opportunity to promote the balanced regulatory initiatives carried on by France during these past three years, and in particular the HADOPI law in the field of copyright, which has recently been supported by the European Parliament, as well as the measures taken to fight the new phenomena of cybercriminal."

Sarkozy, it turned out, intended to use—or to put it more bluntly, hijack—the Paris conference to advocate a Europe-wide version of his "three strikes" law to fight online piracy, despite widespread controversy about the extent to which it erodes legal due process, among other concerns. Dutch Foreign Minister Uri Rosenthal responded with a statement that the Netherlands does not support such laws and that he no longer planned to attend. The conference was "postponed" and never rescheduled. Jérémie Zimmermann, spokesman for La Quadrature du Net, called his president's attempt to hijack the conference "one more example of the alliance between the entertainment industries and a few politicians, who seek to control the public space to remain in power."

Sarkozy was more successful at promoting his agenda eight months later, at a gathering called the "e-G8": an exclusive conference of Internet CEOs, government representatives, and assorted Internet celebrities, organized by the French public relations firm Publicis and held as a prelude to the annual G8 meeting scheduled that year for Deauville, France. Addressing the Internet executives and CEOs in attendance, including Google's Eric Schmidt, Amazon's Jeff Bezos, and Facebook's Mark Zuckerberg, Sarkozy declared, "The world you represent is not a parallel universe where legal and moral rules and, more generally, all the basic principles that govern society in democratic countries do not apply." In a speech not long before the conference, he had said something similar: "The Internet is the new frontier, a territory to conquer. But it cannot be a Wild West. It cannot be a lawless place."

He spoke as if there were no middle ground between total anarchy and the particular solutions he favors. The problem with Sarkozy and

too many other policy makers is not that they object to arrogant, selfish, and irresponsible behavior of companies. The problem is that leaders such as Sarkozy offer a false binary choice between their preferred solutions on the one hand and an anarchic state of nature in cyberspace on the other without allowing for any alternatives. Such a philosophy of Internet regulation is, essentially, neo-Hobbesian: strong nation-state interference to save people from chaos and crime, with the corollary that any rational, responsible citizen should be willing to give up his or her digital freedoms to a trusted authority who knows best.

For the same reason that the world's political thinkers outgrew Hobbesian logic and moved on to Locke, "consent of the governed," and democracy, it is time to consign bipolar Sarkozian arguments for Internet regulation to the dustbin of history. To anybody who believes in democracy (as opposed to anarchy, dictatorship of the proletariat, theocracy, enlightened technocracy, bonapartist autocracy, or some other approach to governance) Internet freedom does not mean Internet anarchy or vigilante justice any more than physical freedom in the democratic context means absence of government. The difference between Internet freedom and Internet tyranny is not *whether* the Internet should be governed; instead it is a question of *how* the Internet should be governed. An Internet that is compatible with—and conducive to—democracy should be governed in publicly accountable ways that reflect the will and respect the rights of the governed. This approach will in turn require an equitable balance of power between government, corporations, and citizens.

Fortunately, some European leaders are still seeking alternatives. In mid-2011 after holding a large consultative conference earlier that spring, the Council of Europe published two documents: a set of principles on Internet governance and a declaration on the Internet's "universality, integrity and openness," beginning with the assertion that "the right to freedom of expression is essential for citizens' participation in democratic processes. This right applies to both online and offline activities and is regardless of frontiers." The objective of the two documents is to ensure that at least within Europe, government laws and regulations, international treaties, and corporate business practices must all be compatible with these fundamental principles to ensure that citizens' rights and interests are not ultimately harmed.

In June 2011, UN Special Rapporteur on Freedom of Expression Frank La Rue delivered a report to the UN Human Rights Council that not only condemned the censorship and surveillance practices of authoritarian countries, but also warned of dangerous trends in the democratic world that threaten citizen rights in the Internet age. He pulled no punches in his critique of efforts by many democratic governments to hold intermediary companies liable for the actions of their customers and users on the grounds that they are in effect delegating the role of censorship and surveillance to unaccountable private actors. "Holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression," he wrote. "It leads to self-protective and overbroad private censorship, often without transparency and the due process of the law."

La Rue stressed the need to preserve citizens' right to online anonymity as a prerequisite for dissent and whistle-blowing, calling on governments to refrain from requiring "real name" registration on social networks, as in South Korea. He was also "deeply concerned" and "alarmed" by French and British "three strikes" laws. Cutting off Internet access as a response to copyright infringement, he wrote, is "disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights." Neither La Rue nor the UN Human Rights Council (of which forty members endorsed La Rue's report) has the power to compel any government to do anything. However, the moral weight of the Human Rights Council has nonetheless helped to shine a global media spotlight on a broad range of governments that threaten Internet freedom. Citizens' groups in various parts of the world will use the La Rue report as a powerful tool in pushing for more reasonable human rights and democratic approaches to Internet regulation.

CIVIL SOCIETY PUSHES BACK

On the eve of the May 2011 e-G8 meeting in Paris, former Grateful Dead lyricist and Electronic Frontier Foundation cofounder John Perry Barlow sent out a tweet quoting Sarkozy: "the Internet is a new frontier, a territory to conquer." Then he added, "And I am in Paris to stop him."

"For the first time in human history, it is possible to convey to every human being the right to know . . . and the right to express him or herself," Barlow later declared from the stage. "This is a very important legacy to give to our children, and if we are going to deny them that legacy on the basis of trying to preserve some old institutions that have outlived their usefulness, we will not be good ancestors." The audience erupted with cheers and applause. Several other academic and activist speakers, invited primarily due to their status as Internet celebrities, pointed out that the people who will drive the Internet's future—users from the developing world, Middle Eastern cyber-dissidents, and the young programmers launching start-ups from their bedrooms—were conspicuously absent, destroying any pretense that the meeting represented the interests or values of anybody other than one group of elites.

Technology blogs and Twitter networks lit up with clever one-liners in defense of an open and free Internet. La Quadrature du Net organized an ad hoc press conference at the end of the meeting to reiterate opposition to Sarkozy's approach. In the end, the calls of activists, academics, and Internet entrepreneurs for an open Internet with minimal regulation dominated news headlines about the meeting. Sarkozy's effort to build consensus around his vision had not gone exactly as planned—because in this important instance, people took action to defend netizen rights and succeeded in bending history, at least a little bit. This success should be an example for other small efforts that can defend an open and free Internet at a time when a series of mostly disconnected initiatives and decisions are determining its fate.

Just as the Tunisian and Egyptian cyber-activists did not spring immaculately from Twitter and Facebook, the La Rue report on the threats to online free expression did not spring forth from a well-oiled

UN research apparatus. Though he drew upon statistics compiled by UN sources such as the International Telecommunication Union, government reports, and information supplied by Internet companies, he also relied heavily on research and policy papers compiled by civil society groups and academics. La Rue also held five consultative meetings in different parts of the world. He heard directly not only from Internet experts, academics, and corporate representatives but also from local activists and online journalists who provided him with first-hand descriptions of the obstacles they face when trying to use the Internet to organize, access information, and disseminate their own reports and ideas.

Also in early June 2011, UNESCO published a report titled *Freedom of Connection—Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. Many of its revelations and concerns were similar to La Rue's, with an added emphasis on a reality that needs to be understood by citizens as well as by companies and governments. "Freedom of expression is not an inevitable outcome of technological innovation," the report concluded. "It can be diminished or reinforced by the design of technologies, policies and practices—sometimes far removed from freedom of expression." Because the Internet is globally interconnected and national governments have failed to offer regulatory solutions that respect and protect the rights of all netizens, they stressed the need for "a stronger multi-stakeholder framework for Internet governance at the international level," with a special emphasis on including free expression and human rights activist groups in the process of setting rules for a new global digital environment. The authors called for the creation of a "special international taskforce for freedom of expression" to better "support and represent these stakeholders in Internet governance."

At a conference soon after the report's release, the Council of Europe's commissioner for human rights, Thomas Hammarberg, accused UNESCO of dodging responsibility. He argued that the United Nations should handle such matters directly rather than handing them off to a task force. As the issue of Internet and human rights moves into the

mainstream and comes into focus for many politicians for the first time, people like Hammarberg are apparently unaware of the history behind UNESCO's recommendation. Frank La Rue did indeed issue an excellent report and set of recommendations—thanks to substantive engagement and hard work in collaboration with academics and activist groups from around the world. But counting on the United Nations as an institution to take practical, concrete steps to protect human rights online has already been proven to be counterproductive.

CHAPTER 13

Global Internet Governance

By 2005, Tunisia under President Ben Ali had already gained a reputation as the Arab world's leading Internet censor. That the United Nations chose Tunis as the venue for a global conference on the future of the Internet could not have been more ironic—or symbolic—of why putting the UN in charge of coordinating the Internet's practical functions would be a setback for freedom of expression.

The World Summit for the Information Society, or WSIS, had three components: first an intergovernmental negotiation over who controls the organizations that coordinate the Internet's global functions; second, a nongovernmental forum with panels and workshops organized by citizens' groups around the theme of "ICT4D," or how to use Internet and communications technologies (ICTs) for economic development; and third, a commercial trade fair in which technology companies from around the world could promote themselves to a global clientele. China's two largest networking companies, Huawei and ZTE (China's second-largest telecommunications equipment maker), were the main corporate sponsors.

Tunisian security forces predictably cleared the roads near the conference hall of ordinary Tunisians. Opposition groups were barred from the proceedings and a number of local activists were arrested. Attempts to hold a parallel international citizens' forum in another part of the city were quashed. The head of the French press freedom group, Reporters Without Borders, was barred from the country. Chinese leaders prevailed

on Ben Ali to ban the New York–based Human Rights in China from entering Tunisia. Of course, the Internet in the conference hall—as in the rest of the country—was heavily censored. Human rights groups pointed out that the UN's choice of Tunisia as host was yet another example of its tendency to lend legitimacy to dictators. It also reinforced the view of many people in the democratic world as well as the global human rights community who believe that control over the Internet's core functions and technical standards should be kept out of the UN's hands.

Thus we face a challenge: if civil liberties are to be preserved and protected, Internet governance cannot be left up to governments alone to negotiate and coordinate among one another. Exactly what the alternative should be, or how it should work, or what success looks like all remain open questions.

THE UNITED NATIONS PROBLEM

In November 2005, I was invited to WSIS by a Dutch foundation to help moderate a discussion and workshop at the nongovernmental forum. Titled "Expression Under Repression," our panel included bloggers from Iran, Zimbabwe, China, and Malaysia; a report on Tunisian Internet censorship by a technologist from the Open Net Initiative; and a hands-on tutorial, organized by my colleague Ethan Zuckerman, for activists wanting to learn how to use the Internet anonymously and evade censorship. Though the UN organizers had approved the workshop and issued conference credentials to all our invited participants, the Tunisian government tried to cancel our event. It did not appear on the official schedule and Tunisian officials informed our workshop's organizers that it was "off topic." Free expression, the Tunisian hosts said, had nothing to do with "ICT for development," the official theme. In the end, the Dutch ambassador had to intervene so we could proceed.

At the appointed time, we found our designated room packed with Tunisian plainclothes police and members of official Tunisian news organizations. As soon as the panelists finished speaking and we moved into a question period with the audience, a woman from Tunisian state

television got up and gave a long speech in French about the arrogance of rich Westerners who lecture people in poor countries about human rights. Countries need to resolve basic issues of food, shelter, and connectivity before they can consider "luxuries" like human rights. I asked our panelists to respond. Activist Taurai Maduna from Zimbabwe silenced the naysayers with a pointed comment: "If we have no freedom of speech, we can't talk about who is stealing our food."

On the other hand, events in Tunisia also underscored just how uneasy many non-Western, developing-world governments feel—including many democratic ones—about a new digital infrastructure that they and their people increasingly depend on, but that is largely engineered and coordinated by people in the economically prosperous West. It is a fact of life that people who have been living in the economically prosperous democratic West all of their lives (no matter how well-meaning they may be) have difficulty understanding and anticipating other people's linguistic and cultural identities—let alone economic and political aspirations. This tension leads to suspicion about what the West's real motives are when it comes to Internet governance and whether the real motives are more about preserving the West's dominance in the global marketplace of goods and ideas than about freedom and democracy that conflicts with those aspirations. This tension is real and needs to be taken seriously if the Internet is going to develop in a manner that will serve the fastest-growing segment of Internet users—who happen to live in non-Western, largely non-English-speaking countries.

This East-West imbalance was one of the many reasons cited by the Chinese government in its 2005 bid to remove control over critical Internet infrastructure from US government and private, largely Western, hands. Up until the late 1990s, the system coordinating Internet domain names and IP addresses—a system that ensures, for example, that when a person types www.cnn.com into the address bar on a browser, that person gets the same website everywhere—was handled through a largely informal process by a group of engineers living mainly in the United States. In 1998, this coordination function was formalized with the establishment of a San Diego–based nonprofit corporation called

the Internet Corporation for Assigned Names and Numbers, ICANN. Its budget comes primarily from the fees collected through the sale of domain names. Technical and policy decisions are made by a board of directors in consultation with various "constituencies" of network engineers, corporate interests (companies that either administer, sell, or use domain names), Internet user groups, and governmental representatives, through an elaborate system of councils meant to balance out the interests of the Internet's different stakeholders.

Under ICANN's original governance structure, the US government had no role in the organization's day-to-day decision-making. But because the Internet had by then become so important for the American economy, ICANN was required to sign a memorandum of understanding in which it committed to ultimate oversight by the Department of Commerce. This relationship led to mounting concerns by other governments over the past decade as the Internet became more important—indeed critical—to more countries. Many governments were uncomfortable with the idea that the United States had direct power over such a vital if still young global system. Given the frequent tensions plaguing US-China relations and the strategic emphasis it places on technology, the Chinese government was particularly uncomfortable. But so too were the Russians and the Iranians, as well as others including democracies such as Brazil and even some in Europe.

In the run-up to the 2005 Tunis meeting, the Chinese government led a bid to dismantle ICANN and transfer its functions to a UN body, the International Telecommunication Union (ITU). Many developing-world governments supported this plan because they have more power in the ITU, where all countries have equal voice, no matter whether they are represented by engineers or by diplomats who may or may not understand the technical complexities under discussion. At ICANN, the perspectives of Western engineers and Western companies have tended to dominate, especially in its early years—and those lacking technical understanding have been paid little attention.

Despite recognizing that this digital divide does not serve the interests of developing-country Internet users, human rights and civil liberties

groups from all over the world have been united in opposition to any plan to transfer control over critical Internet resources from ICANN to the United Nations. Such a move would empower governments that routinely practice political and religious censorship. Dictatorships would gain greater influence over the Internet's regulatory and technical norms in ways that could potentially undermine or imperil dissenters and unpopular minorities who use the Internet all over the world. The United States stood with the human rights groups, which was not difficult since human rights principles conveniently overlapped with the US self-interest in keeping ICANN under its umbrella rather than handing it off to the UN. The Europeans sought a middle ground by which ICANN's oversight would be more international but not directly under UN control either.

In the end, diplomats at the World Summit agreed to disagree and to maintain the status quo. ICANN was left alone, but with an admonition to become more international and inclusive, which it has subsequently attempted to become by bringing more governments into its multi-stakeholder consultative policy process. Meanwhile, the UN delegates agreed to create a new talk-shop, the Internet Governance Forum (IGF), where governments, companies, and NGOs from all over the world now meet annually to discuss Internet policy issues.

Though the IGF has no power to set policy or make binding decisions, it does provide a forum through which governments, companies, and NGOs from all over the world can identify common problems, disagreements, and solutions. Over the past six annual IGF meetings, many transnational "public-private partnerships" have emerged to handle issues like cyber-crime, the digital divide, and child protection. In his book *Networks and States*, Internet governance scholar Milton Mueller of Syracuse University argues that the IGF, if organized and managed well, has the potential to serve as a global "coral reef," supporting a whole ecosystem of formal and informal "policy networks." Through these networks that are formed or broadened through IGF participation, professionals working for different governments, companies, and NGOs can forge ties that enable them to solve problems for the world's Internet users in flexible, ad hoc ways.

One of the IGF's many problems is that it is dominated by whichever governments, companies, and organizations have the financial resources to participate. Governments from the developed world are well represented at the IGF, while participation by those from poorer countries is generally patchy. Governments with clear agendas on Internet governance issues such as China, Iran, India, and Brazil position themselves as representing the interests of the non-Western "Global South." Corporate interests are mainly represented by the major Western multinationals plus a few other large players from China, Japan, and India. Nongovernmental interests are represented primarily by international NGOs based in Western countries, plus some from India and a few of the better-resourced democratic African countries with active technical and engineering communities, such as South Africa, Ghana, and Kenya. Nongovernmental voices from authoritarian countries are almost entirely absent. As a result, only the governments—or government-approved so-called nongovernmental organizations—speak for the interests of Internet users in those countries.

In 2009 the IGF was held—ironically once again—in Sharm El-Sheikh, Egypt, the resort city where former president Hosni Mubarak maintained a home and where he and his wife were held under house arrest since the February 2011 revolution. Little did the IGF participants imagine that in just over a year, Mubarak's regime would be brought to its knees by Internet activists—none of whom were invited to the meeting.

An entire morning of the four-day forum was disrupted by an unscheduled speech given by First Lady Suzanne Mubarak, who wanted to promote her Cyber Peace Initiative for online child safety. Intel was a major sponsor of her initiative. Family safety organizations from the United States and Britain rushed to sign partnership agreements with Mrs. Mubarak's organization. At one point during the meeting I asked members of one prominent British child safety organization if they knew about the Egyptian government's record of arresting and torturing young Egyptian bloggers and Facebook users critical of Mubarak. They were not. I asked if they knew that child safety is commonly used by authoritarian regimes as an excuse for censorship and surveillance.

Two people who play leading roles in their organization expressed great surprise and discomfort. It was clear that they had not considered these issues, or how they might inadvertently be lending legitimacy to a regime that does not respect human rights.

As a speaker on a panel about social networking services, I planned to cite Egypt's record of jailing and torturing bloggers, China's system of corporate-level censorship, and South Korea's real-ID requirements, among other cases. Just beforehand, Nitin Desai, a UN undersecretary-general and chairman of the Internet Governance Forum, took me aside and warned me not to mention any UN member countries in my remarks. Otherwise, since this was a UN meeting he would have to give all governments the right of reply, which would use up all available time and prevent the panel discussion from proceeding. Earlier during the conference, the Open Net Initiative had been confronted by UN security after it tried to display a banner in the hallway advertising a launch event for *Access Controlled*, a book about global censorship. According to the security guard who removed their poster, a certain UN member country had complained because the ONI had not obtained permission from the IGF secretariat to display the poster.

As an organization formed to coordinate policy between nation-states, the United Nations has clearly struggled to run a process aimed at ensuring that the Internet evolves in a manner that benefits all stakeholders—an Internet that people around the world can reasonably trust to protect their rights or defend their interests. The most problematic aspect of the IGF is the charade perpetuated by many of its most powerful participants that it actually is a neutral and fair discussion platform through which governments, companies, and citizens' groups can discuss common problems of the digital realm. So far it has fallen well short of this description.

ICANN—CAN YOU?

In December 2010, ICANN CEO Rod Beckstrom gave an impassioned speech at the United Nations defending the multi-stakeholder

model as more compatible with the Internet's intrinsic nature than any kind of global governance system based on nation-states. ICANN, Beckstrom argued, is proof of how well "the multi-stakeholder model works." He was certainly right that the nation-state system is not the appropriate framework for governing the Internet. The truth is, however, that ICANN's multi-stakeholder process is an early-stage experiment. ICANN works much better for some countries, companies, and Internet users than it does for others. Though its multi-stakeholder decision-making model means that even some of the world's most powerful governments do not always get their way, ICANN has not yet figured out how to serve the interests of all the world's netizens fairly and efficiently. Until it does so, its claim to sovereignty over even one specific function—coordinating the Internet's critical addressing and numbering resources—will remain vulnerable to attack from many different sides.

In June 2009, I attended one of ICANN's public meetings, held three times a year for a week in a different part of the world. This one was in Sydney, Australia. Every meeting includes a public comment session: an opportunity for anyone attending the meeting (which is open to literally *anybody* who signs up) to raise concerns and questions directly to the board of directors. Twenty board members sat on a raised platform at one end of the Sydney Hilton's grand ballroom, gazing out from the dais at several hundred men and women, many sitting with laptops open.

A dozen or so people lined up behind two microphones placed in the aisles, taking turns to ask questions and make statements. Eventually an American woman with close-cropped silver hair took her turn. "My name is Marilyn Cade," she said. "I'm speaking as an individual and have appeared before this council of master Yodas many times. . . . I use the term master Yodas because I think, in fact, I understand that we are asking you to exercise wisdom."

Cade worked for AT&T for many years and is now an independent consultant who is heavily involved with the politics of both the IGF and ICANN. The specific issue she raised that day had to do with the board's right to appoint a panel of experts to study a question related to intellectual property and domain names. But the larger point

is that, apart from the absence of any known extraterrestrials, her analogy between the ICANN board and the *Star Wars* Jedi Council was apt. The men and women on the dais are stewards and protectors, not of "the Force," but of the Internet. Unlike the Jedi Council, they are appointed with term limits. Like the Jedi Council, the source of their power and legitimacy is fuzzy. Their authority will last only as long as the bulk of the world's network engineers and most governments choose to respect it.

ICANN's function is narrow but critical. It runs the world's domain name system, or DNS. Most people who use the Internet do not need to know anything about the DNS, thanks to the people and organizations around the world who make it work smoothly. Web pages, e-mail, and other applications hardly just float in space; their data actually resides on computer servers physically located somewhere. When you type a web address into your browser, you expect to get the same website no matter what kind of browser or device you are using, and no matter where in the world you happen to be. When you send an e-mail to a particular address, you want it to go to the same person no matter where in the world you're sending it from and where that person is located. Every computer server or network has an IP address. The trick to making everything work is to make sure that all of the domain names used by everybody all over the world all correspond to the same IP addresses. If there is a discrepancy, then a single globally interoperable Internet will be "broken."

IP addresses also have to be allocated. The original IP address system was based on sequences of four numbers, known as IPv4. Nobody imagined when the Internet was created that those numbers would run out, but they did in 2011. Now the world's entire technical community is managing a transition to a new system based on six numbers, called IPv6. Somebody has to allocate and keep track of the distribution of IP addresses—whether they are "v4" or "v6." Currently that job is done by an organization tied to ICANN called the Internet Assigned Numbers Authority (IANA), which allocates blocks of IP addresses to five regional Internet registries (RIRs), one for each of five regions of the world. The

RIRs are run by networking engineers from all the countries in each corresponding region; large organizations such as universities, banks, and Internet service providers (ISPs) and any other organization requiring large numbers of IP addresses pay to become members of their local RIR. These RIRs hold regular meetings, at which engineers discuss technical problems and make consensus-based decisions about solutions. The global system works because all of these engineers have agreed to trust one another and honor their regional RIR's decisions.

Though governments and government-affiliated organizations around the world are involved with the RIRs and engineers from all over the world help run them, the system is not controlled by governments—with one big exception: IANA is under contract with the US Department of Commerce. Herein lies the core issue that many other countries, especially China, object to so strenuously. There are periodic moves to wrest control over IP address allocation and domain name system coordination away from IANA, the other RIRs, and ICANN and put these functions under governmental control through the UN's International Telecommunication Union or similar. The UN system's chronic inability to protect and uphold human rights around the world, and its propensity to empower and legitimize dictators within the global governance system—as well as the lack of technical understanding of how the Internet really works among many countries' ministers of communications—are good reasons that power over the Internet's critical resources should be kept out of intergovernmental hands.

But as the Internet's importance grows, and as a critical mass of the world's Internet users expands far beyond its original core of affluent Westerners to include much less affluent people on mobile devices, and people who read and write only Chinese, Arabic, Urdu, Japanese, Korean, Russian, one of India's eighteen official languages, or anything else that doesn't easily "interoperate" with the English-language alphabet, the strains and stresses of Internet governance are mounting. ICANN is struggling to manage these strains in a way that facilitates the Internet's development, and in a way that genuinely works well for all of its users, not just for the wealthiest English-speaking ones.

Why should people who are not network engineers care about these seemingly obscure issues of Internet governance? Most of the world's Internet users have never heard of ICANN, the DNS, or RIRs, or any of the global power struggles taking place within and around these and many other acronyms. The outcome of these power struggles, however, will affect the extent to which dissent and unpopular speech—or any speech that displeases powerful governments or large brand-name corporations—can have safe passage and a safe home on the Internet. Many of the actors in these power struggles claim to be representing the interests of people who have no idea that they exist, and who likely would not trust them if they were aware.

A lot of the recent politics around the DNS have to do with who controls domain names and who makes money from them. Until 2010, all domain names were in Roman letters only—if your native language was Chinese or Arabic, tough luck, you still needed to be sufficiently familiar with the Roman alphabet and to know how to type Roman letters or you couldn't use the Internet. That started to change in 2011 when ICANN rolled out what are called "internationalized domain names," or IDNs. Every country gets what's known as a country-code top-level domain (ccTLD in ICANN acronym-speak), such as .cn for China or .uk for the United Kingdom or .ca for Canada. Starting in 2011, countries with the technical ability to manage the process could also register IDN ccTLDs. Egypt and several other Arabic-speaking countries rolled out Arabic top-level domains so that businesses and organizations in their own countries could register web addresses entirely in Arabic, making them accessible to more people for whom the English alphabet is completely alien. China, Korea, and Japan have all rolled out similar IDN variants of their country-code top-level domains. Since domain names are sold to individuals and corporations for money, this linguistic expansion of course is a great business opportunity for a whole industry that has grown up since the 1990s around enabling people to purchase and trade domain names.

Domain names like sex.com and business.com have sold for millions of dollars, benefiting the tech-savvy first-movers who grabbed lucrative

domains in the 1990s before most businesses realized how important these names would become for them. In June 2011, after several years of disputes and bargaining among the organizations and various constituencies, the ICANN board decided to expand the Internet's real estate even further by allowing any organization with enough money and technical capacity to apply for new generic top-level domains (gTLDs). Companies will be able to create top-level domains for their brand (.ibm, .apple) and cities can create top-level domains for themselves (.seattle, .berlin, .beijing)—and all of these things can be done in any major language or script on earth. ICANN will charge a five-figure registration fee for the privilege of running and administering a top-level domain name, plus annual fees on top of that.

This is a lucrative opportunity for all concerned: it gives people an opportunity to create virtual real estate out of nothing and then sell it. For example, a business or organization serving people surnamed MacKinnon could in theory (assuming they can afford the $185,000 application fee and a further annual fee of $25,000) apply to run the .mackinnon gTLD. That way, instead of buying rebeccamackinnon.com, I could purchase http://rebecca.mackinnon from a domain name registrar. If a coalition of people of Scottish descent wanted to apply for ownership of the .mac gTLD as a community-building or moneymaking venture, however, we would run into trouble. Apple owns the trademark for "Mac."

Control over property and real estate in the physical world has always been the focus of complex and heated politics—in fact, resistance to the king's arbitrary power to confiscate land and property was the main impetus of the Magna Carta and subsequent basis of "consent of the governed" in modern times. Power struggles over control of land and property have always been at the core of politics and geopolitics. Now those struggles have entered a new dimension with the Internet.

Digital real estate is turning out to be as political as physical real estate, with the added complication that the network is borderless and global, which means that the politics of digital domains are waged simultaneously within countries and across many borders. The political

and commercial clashes of the physical world are remixed and recast in complicated ways. Some kinds of businesses and other constituencies of Internet users stand to gain from the expansion of Internet domain names; others believe they have much to lose as ICANN moves ahead with the new gTLD program.

Chief among the potential losers are large Western multinational companies with internationally famous trademarks and brands, which lobbied heavily against the domain name expansion. Back in the 1990s, there were famous cases of "cyber-squatting," whereby tech-savvy and opportunistic individuals registered domain names of famous brands, followed by .com, and demanded high sums of money from the companies. In other cases, legitimate disputes arose over who had the right to a particular domain: Volkswagen went to court over vw.com, which had been registered first by a small company in Virginia called Virtual Works. The court ruled in Virtual Works' favor. Thus many name-brand companies fear that a potentially unlimited number of new gTLDs will bring new costs to "own" all domain names related to their brands, compelling them to act quickly every time a new gTLD is launched, buying up thousands more domain names related to their brands, and when necessary suing for ownership of domain names they believe are rightfully theirs.

After the ICANN board decided in 2008 to begin laying the technical, legal, and political groundwork to launch new gTLDs, an intense battle ensued over who has a right to apply for any given name in any language, how the application process should be run, what criteria should be used for acceptance or rejection, and who, if anyone, gets veto power. Governments concerned about the use of certain names to promote dissident platforms or content deemed offensive demanded veto power over applications. Companies concerned about protecting their trademarks and brand names (known within the ICANN world as the "intellectual property" constituency) advocated strict controls preventing anybody except brand owners from registering any names in any language that resemble their brands. Many Western governments, lobbied heavily by those companies, supported their position.

On the other side of the argument, civil liberties groups and consumer rights advocates countered that giving veto power to governments and corporations over new domain names would chill free expression. Companies and governments from the developing world argued that excessive trademark and copyright protection measures being pushed by major Western multinationals would discriminate against less globally famous, non-Western companies with a following in their own communities but whose brands may have names similar to those of major multinationals.

ICANN's board makes the final decisions, but it takes policy recommendations from a number of councils and supporting organizations that deliberate via conference call, e-mail, and in-person meetings. These councils and supporting organizations consist of people claiming to represent different constituencies (noncommercial users, consumer groups, commercial registrars and registries, trademark-holding companies, engineering interests, etc.). Governments participate in an advisory role only, through what is called the Governmental Advisory Committee (GAC). No government representatives sit on ICANN's board of directors, which has demonstrated clear independence from the world's most powerful governments, including the United States. In June 2011 the United States and the European Commission led an effort to force ICANN to delay the launch of the new gTLD program, due to what they felt were unresolved trademark and commercial concerns. The ICANN board, confident that the rules set out for the new gTLD program were the result of a consensus developed over years by a diverse set of stakeholders, ignored the objections from Washington and Brussels and approved the program anyway. Among those applauding ICANN's defiance was Eliot Noss, CEO of the Canadian company Tucows, which sells domain-name, e-mail, software, and small business services, who commented after the board vote that "if you're talking about the Internet, nations and nation states are just actors at the table, not predominant."

Non-Western governments also complain that ICANN's multi-stakeholder structure contains a Western-centric bias because the organization is dominated by people from the Western developed world. The working language is English, with representation by businesses and nongovernmental organizations too geographically narrow to reflect the full range of concerns and challenges of Internet users in developing countries where most of the Internet's expansion is now taking place. Because of this imbalance, a growing chorus of governments—with China in the lead—have demanded that ICANN elevate the role and influence of the GAC in the organization's decision-making process so that their people's interests can be better represented.

Unfortunately, the authoritarian and quasi-authoritarian governments active in the GAC are even less interested in defending the right to free expression and privacy of their citizens than the Western governments are. At least businesses and nongovernmental groups from democratic countries can openly oppose their own governments' positions at ICANN. Entrepreneurs and civil society groups from countries where open defiance of the government is not tolerated cannot come to ICANN and advocate for positions that clash with their government's. Thus, even though ICANN claims to be a multi-stakeholder body with a bottom-up approach to its decision-making and policy-making processes, in reality the interests of Internet users from authoritarian countries are represented only by governments, businesses with close governmental ties, and quasi-governmental organizations. The interests and rights of dissidents, politically unrepresented minorities, and cyber-activists from nondemocratic countries have no meaningful representation at ICANN from any quarter, except indirectly from the very few international human rights and free-speech groups with the staff, resources, and expertise to engage in ICANN policy-making processes.

In 2009 Global Voices, the grassroots citizen media network that I cofounded, became a member of the Non-Commercial User Constituency of ICANN's Non-Commercial Stakeholder Group (NCSG). The NCSG was created to represent the interests and defend the rights of people around the world who use the Internet largely for noncommercial purposes, which of course includes political activism. Ironically, noncommercial users have had to fight hard within the ICANN bureaucracy and

arcane governance structures to gain fair representation within what is billed by its leadership as a bottom-up, grassroots, and inclusive decision-making process.

In 2009 the NCSG was told that in exchange for six seats on one of the stakeholder councils that make policy recommendations to the board, it would be allowed to elect only three of those seats, with the remaining three noncommercial user "representatives" appointed by the board. The NCSG was not allowed to write its own governance charter but instead had one imposed by ICANN staff. "Welcome to 'bottom-up' policy making at ICANN," remarked Robin Gross, constituency chairperson at the time. Milton Mueller reported on his blog, "Apologetic Board members openly confessed that they did this simply to appease the commercial user groups who, they feared, would 'go ballistic' and create trouble for them in Washington if they did not."

Over the ensuing two years, representatives of the beleaguered noncommercial constituency—most of whom participate in ICANN as unpaid volunteers, unlike corporate representatives to ICANN whose companies pay for their participation and consider it part of their jobs—negotiated and bargained with the board and ICANN staff for a more favorable charter, including the right of its members to elect all of their representatives. The NCSG also continued to challenge the ICANN board and staff regarding weak representation from "developing and transitional" countries. In response to such challenges from NCSG and others, ICANN has improved its "remote participation" tools, which enable people from around the world to follow and participate in meetings through the Internet and by phone. ICANN has also expanded a fellowship program for "individual members of the Internet community who have not previously been able to participate in ICANN processes and constituent organizations." Much more will need to be done, however, if the interests of all the world's netizens are to be fairly represented at ICANN.

Certainly, when it comes to upholding human rights and free expression, the UN governance model is far worse. It is clear that it is not in the interest of the world's netizens to leave Internet governance to

nation-states. Yet the structures and processes that have so far been built for multi-stakeholder Internet governance are failing to mediate the kind of global politics needed to uphold and protect human rights, civil liberties, and free expression in the global network.

Meanwhile, ICANN lumbers on, despite accusations from all sides of ineffectiveness, waste, mismanagement, and questionable legitimacy. Milton Mueller points out that multi-stakeholder institutions like ICANN have their own form of international, multi-stakeholder "pluralist politics" that allow for various stakeholders to speak and be heard and to lobby for their interests—assuming they can afford to participate both in terms of time and in terms of resources to attend meetings (and the political risk if they are trying to represent nongovernmental interests of people in authoritarian countries). The problem is that this multi-stakeholder political process takes place without a basic values framework—at a national level often called a constitutional framework—that would prevent political outcomes from violating the rights of some Internet users in various parts of the world, because either they are on the losing side of a bargaining process or their concerns are not even represented or understood. Mueller rightly concludes, "There can be no cyberliberty without a political movement to define, defend, and institutionalize individual rights and freedoms on a transnational scale."

The next step is to build that movement.

CHAPTER 14

Building a Netizen-Centric Internet

Almost six months to the day after the ouster of Tunisian president Zine El Abidine Ben Ali, a small protest of roughly 150 people formed in the middle of Tunis.

"We are all Samir Feriani," the protesters chanted, brandishing photos of the forty-four-year-old police officer. Feriani had been arrested two weeks previously after writing to Tunisia's interior minister, naming several high-ranking ministry officials who he said were responsible for killing protesters and committing other human rights abuses during the Tunisian revolution. In one of the two letters published in a local magazine, he further claimed that ministry officials had been destroying sensitive archives since Ben Ali's ouster, including archives of the Palestinian Liberation Organization (based in Tunis from 1982 to 1994), which he said documented Ben Ali's relationship with Israeli intelligence. Feriani was charged with "harming the external security of the state," "releasing and distributing information likely to harm public order," and "accusing, without proof, a public agent of violating the law."

Tunisia's twitterati clamored to support Feriani, dismayed that elements and behaviors of the old regime lingered on in the new Tunisia. "Where are our journalists, the civil society and the political parties?" asked a Twitter user called @emnamejri. On Facebook, people created pages calling for his release. They posted pictures of protests, links to

news about his case, and aggregated reactions of citizens around Tunisia. They circulated the condemnation by Human Rights Watch, which summed up many people's feelings about his arrest: "At a time when many Tunisians believe that the officials who terrorized people under Ben Ali remain strong within the security establishment, the provisional government should be encouraging whistle-blowers, not using the ousted government's discredited laws to imprison them."

At a conference in New York about the Internet and politics that same month, somebody asked Riadh Guerfali—the activist who made the 1984 Ben Ali mash-up back in 2004—whether he was worried that the Tunisian revolution would not end well. "I am optimistic that we will win this battle," he said. "At the present time there is still lots of trouble," he continued. "But public opinion is here." Despite the steep uphill battle, the difference between then and now is that Tunisians have carved out a space in the media and on the Internet for discourse and debate that is vastly broader and more accessible than under Ben Ali. "If we can say, this is wrong, we can say the person responsible must resign," that is the first step, Guerfali told the room full of young American political operators, bloggers, journalists, and techies. "Things never ever, anywhere in the world, change by itself. It takes the pressure of public opinion."

This truth applies to everyone, everywhere. Democracy will not be delivered, renewed, or upgraded automatically, like the latest Netflix blockbusters through our broadband connections and smart phones. The future of freedom in the Internet age depends on whether people can be bothered to take responsibility for the future and act. Just as our individual actions and choices as citizens, parents, teachers, employees, managers, and government officials combine to shape the kind of world we live in, the actions and choices of each and every one of us are shaping the Internet's future.

Elements of a transnational movement to defend and expand Internet freedom have begun to emerge. Like the Internet itself, this movement is decentralized, loosely if at all coordinated, and driven often by groups and individuals at the edges reacting to specific problems. For now the movement is neither sufficiently broad nor sufficiently powerful to keep the abuse of power by governments or corporations systematically in check. But the revolutions, and attempted revolutions, of early 2011 have jolted many more people around the world into becoming actively engaged with the power struggle for freedom and control of the Internet.

What should this movement be aiming for? Establishing some sort of global UN-like uber-government to manage and restrain cross-border digital power is neither realistic nor desirable. Nor is Robin Hood–style cyber-vigilantism and digital guerrilla warfare. Given human nature and the realities of today's world, it is also inconceivable to expect to start completely afresh with some sort of utopian digital democracy in a pristine and politically unspoiled frontier of cyberspace.

A more realistic and democratic approach is to build and strengthen alternative netizen-driven institutions and communities that can exist alongside existing ones, eventually shifting the balance of power both online and off. At the same time, we must devise more effective and innovative ways to constrain all forms of digital power within reasonable limits, whether that power is exercised by governments, corporations, or activist hacker networks of varying ideological and religious stripes. The first step is to build much broader public awareness and participation. People need to stop thinking of themselves as passive "users" and "customers," and start acting like citizens of the Internet—as "netizens."

STRENGTHENING THE NETIZEN COMMONS

Rosental Alves, a Brazilian journalist who now heads the Knight Center for Journalism in the Americas in Austin, Texas, likes to compare the pre-Internet age to a desert. Most people had easy access to a very limited number of sources for news and information. People's understanding of the world depended on the priorities and budget decisions of the editors who ran news organizations, and whatever or whoever could influence them.

Then came the deluge. Today we live in an informational rain forest that sprang up around us practically overnight. We were not prepared

for such an overwhelming ecosystem of rapidly evolving info-organisms. We have moved abruptly from a problem of scarcity to a problem of overabundance, at least for some varieties of information. Others are scarce and harder to find, drowned out or buried amid the rapidly proliferating dominant species. The bulk of online media are now things that we produce ourselves—on social media, on blogs, on personal websites. Journalists and media professionals now compete for attention and influence one another. "The logic of communication that is being created in this new era is based on engagement," Alves says.

Many elected officials of the world's major democracies complain about the low quality, viciousness, or navel-gazing nature of much of the discourse they see online. What many of the complainers seem not to recognize is that unless they want to destroy freedom of speech and anonymity on the Internet through overregulation and unrealistic demands on companies to police the citizen-created content they host and transmit (in which case they are enemies of freedom regardless of whether they intended to be), the only answer to bad speech is better and more effective speech.

Of course, just because anybody can now create and transmit media does not automatically mean that human society will be more democratic or peaceful. Life in the rain forest is just as likely to be nasty, brutish, and short, a Hobbesian state of nature that is not only primeval but also primitive. In the offline world, this is why we build civilizations. It is now up to the world's netizens to figure out how to build a sustainable civilization within the new digital rain forest—in which we find sustenance and shelter amid the poisonous plants and deadly predators.

Success is by no means inevitable. People still need to learn how to participate constructively and responsibly in this new space and protect the rights of minorities and dissenters. The right incentives and disincentives for good and bad behavior online have yet to be worked out. Solutions that adequately protect netizen rights will come about, however, only if netizens of the world participate actively in devising them. The more we actively use the Internet to exercise our rights as citizens and to improve our societies, the harder it will be for governments and

corporations to chip away at our freedoms, arguing as they so often do that we do not deserve them, and treating us like reprobates.

Global Voices is one of many emergent communities of people who assert their citizenship of the Internet, not as passive users or consumers. They take personal responsibility for the future of online information—and its freedom—by contributing directly. There are many other such communities dedicated to building a new kind of civilization that will be better suited to our young and rapidly evolving digital rain forest, communities that do not insist upon maintaining the old desert ways of life, along with all the institutions and customs that made sense in the old context but may doom us in the middle of a deluge. Wikipedia, the encyclopedia that anybody can edit, is perhaps the most famous example of an information resource that anyone on earth can contribute to, but that is maintained and governed by a core community of people around the world who believe in the idea that elites no longer control human knowledge. They have proven that a group of people with a common set of objectives can govern themselves according to a set of community rules and produce a resource that no amount of public funding or corporate revenue can come close to creating.

Equally important are the more locally focused citizen media organizations dedicated specifically to document, call attention to, and take action against violations of citizens' digital rights. The Tunisian website Nawaat.org, run by Sami Ben Gharbia, Riadh Guerfali, Slim Amamou, and others, served as an anchor for the Tunisian digital activist community. Though they also used commercial platforms like Facebook, Twitter, YouTube, and Flickr as key components of their activism strategy, Nawaat.org served as a one-stop consolidator and archive of information. It also served as an important backup when commercial services were blocked or accounts were hacked or shut down. In Egypt, websites like the Torture in Egypt blog and the Egyptian Blogs Aggregator run by open-source programmer Alaa Abd El-Fattah similarly served as anchor points for more diffuse campaigns over multiple social media sites, which had broader reach but over which the activists themselves had less control in terms of how the information was stored and shared.

Another type of organism in the new ecosystem is Creative Commons, a nonprofit founded by Lawrence Lessig—then at Stanford, now at Harvard—dedicated to helping people share information and media, as broadly or as narrowly as they would like. Its flexible system of copyright licenses enables organizations like Global Voices, Wikipedia, and many other nonprofit citizen projects to ensure that their content is shared as widely as possible and translated into as many languages as possible, with the creators' full approval and consent. The point is that people who want to protect their works with traditional copyright certainly can, but many other people who create media for reasons other than sales should also be able to do so.

Other groups are focused explicitly on keeping the Internet as open and free as possible. In 2009, Mozilla (creator of the Firefox browser and other open-source tools) launched Drumbeat, a platform through which people can become actively involved in keeping the web open and free by organizing their own projects and recruiting others to help. One team is working to develop a set of universal "privacy icons"—a set of symbols that companies could adapt, which would make it easier for users to understand what personal information is being stored and for how long, and how and with whom it might be shared, under what circumstances. That in turn would make it easier for a user to decide how to use—and not use—any given service. Several other projects focus on creating free courses, instructional manuals, and other educational tools so that nontechie web users can improve their web literacy and ability to build and modify one's own tools. The point of the Drumbeat movement is that the web will be free and open only if people participate actively in making it so.

Still others focus on educating netizens about how they can protect themselves from threats to their freedom. Global Voices Advocacy works with a range of other nonprofit organizations to disseminate information in a range of languages about the threats citizens face to their freedoms and rights online, and what tools and tactics they can use to protect themselves. The Tactical Technology Collective develops training materials for citizen privacy and security, while Mobile Active in

turn works with a network of technologists and activists to help people fight censorship and surveillance on mobile phones.

EXPANDING THE TECHNICAL COMMONS

When the Egyptian government shut down the Internet on January 27, 2011, a worldwide community of activist programmers and engineers—"hacktivists"—sprang into action. Internet and mobile service providers in Egypt were down, but as long as there were phone and fax machines capable of making and receiving international calls, there were still ways for Egyptians to connect to the Internet. The most famous effort was a collaboration between Google and Twitter, called "Speak to Tweet": people could find a landline, call a phone number, and record a message that would then be disseminated to the world through Twitter.

Other efforts actually enabled Egyptian activists to connect directly to the Internet despite the blackout. Members of a loosely organized group called Telecomix, originally formed in Sweden and now with hundreds of active members around the world, along with its operational sister organization called We Rebuild—both dedicated to promoting "access to a free Internet without intrusive surveillance"—began collecting information about dial-up Internet services in Europe and other countries in North Africa and the Middle East that Egyptian people could access from any landline with international service. It was an expensive call, but at the height of a political crisis it was better than nothing. The hacktivists then searched the Internet for Egyptian fax numbers and began faxing the information as far and wide as they could. They also put up a website on which they updated new dial-up information regularly, and distributed that to expatriate Egyptians, who then called the landlines of friends and relatives, who could then pass on the information. A small French ISP offered the free use of its dial-up service by Egyptians. Other such accounts were purchased from services around Europe and North America by supporters of the Egyptian revolution living around the world.

A range of activist entrepreneurs, nonprofits, and foundations are now looking for ways that activists can be more prepared, whenever and

wherever the next government flips the "kill switch." Soon after the Egyptian shutdown, a consortium of developers, led by the New America Foundation's Open Technology Initiative, began integrating a number of existing open-source platforms into easy-to-use software that can be installed on almost any device with a Wi-Fi connection, so that in the future when a government blacks out the Internet, activists will at least be able to remain connected to one another by linking together their laptops and Wi-Fi-enabled mobile phones in a local "mesh" network. Dubbed Commotion Wireless, a core component of the project is a software program called Serval, which enables people to create an ad hoc independent cell phone network using their existing phone numbers, even when the normal commercial networks are destroyed or switched off. A Serval-based network has already been deployed successfully as a test case in the Australian Outback. Data are stored within the local network for relay onto the Internet when and where a connection can be established at least occasionally. (The project received funding from the State Department in spring 2011.)

The idea of mesh networking is not new. Civic-minded engineers and software developers have been working for more than a decade to address the problems caused by the combination of government and corporate control over both how, and whether, ordinary citizens can access the Internet. The community wireless movement first emerged in North America and Western Europe as part of an effort to provide access to remote and economically disadvantaged citizens whom corporate Internet and wireless carriers have little or no business incentive to serve. The largest and most successful community wireless project is Guifi.net, which started in Catalonia and has expanded into other parts of Spain's Iberian Peninsula where rural households have not been reached by Telefonica, the main Spanish telecommunications company. Other projects are under way in Berlin, Vienna, and Athens. In Detroit an organization called the Digital Justice Coalition is promoting community-owned broadband and wireless services that prioritize locally produced content as a way to promote community, local innovation, and civic involvement. An important component is local mesh networking within neighborhoods: one resident or business obtains a commercial Internet connection, then that signal is shared or relayed throughout the neighborhood by inexpensive routers in each house. A whole community of software and hardware innovators has emerged around these projects, sharing software code and hardware designs, and learning from one another's successes and failures.

In authoritarian states and bonapartist quasi-democracies, community-controlled connectivity is difficult to establish, let alone maintain without reprisal, and is thus likely to emerge only in situations involving open revolt and rebellion. In democracies, local connectivity movements are still so small and new that their broader political implications remain untested. Proponents of community wireless and neighborhood mesh networks are working to ensure that laws, regulations, and technical standards can enable community wireless to thrive and coexist alongside—and even sometimes in symbiotic relationship with—existing corporate services. In a time when it is becoming increasingly difficult for people to participate fully in politics and political discourse, start a successful small business, or avail themselves of government services without Internet and wireless connectivity, we netizens should be free to organize alternative means of connectivity when commercial options fail to meet our needs.

For people seeking to evade censorship and surveillance on whatever network they happen to be using, activist software developers have been working for years on a range of tools. A range of software developers with different commercial and non-commercial affiliations have developed software tools that help Internet users in China, Iran, and other authoritarian countries to access blocked content. Some are more effective and secure than others. One group of open-source engineers has spent the past decade working on an "anonymizer" tool called Tor, which enables users to surf the web and upload or download content without being traced. Between the start of the Egyptian protests on January 25, 2011, and the blackout on January 27, the use of Tor from Egypt more than quadrupled, due to activists' concern about police surveillance of their Internet communications. Developers are also working to bring

secure Internet access with Tor and other tools to mobile phones, or at least those using Google's open-source Android operating system. Some countries, such as Iran and China, have figured out how to block Tor's publicly known channels, creating an arms race in cyberspace between activist developers and government engineers.

Other activist engineers and programmers are working on the problem of corporate control of our social and political lives online. In 2010 at the height of negative publicity about Facebook's privacy policies, four young programmers from New York University's Courant Institute launched an open-source project called Diaspora, which aims to provide a software download or "pod" that people can install on their own computer servers to create their own Facebook-like social networks. Rather than having Facebook controlling people's personal information and policing users, the idea is for decentralized groups to be able to control their own platforms and data. Their online drive to raise $10,000 that summer garnered so much interest that they ended up raising nearly $200,000. A group of programmers in the Seattle area has developed open-source social networking software called Crabgrass, tailored specifically for the needs of political activists. An older project, StatusNet, enables people to set up their own Twitter-like microblogging services that they can control locally.

In early 2011 Columbia University professor Eben Moglen announced a new project dubbed FreedomBox, aimed at addressing the vulnerability of activists and dissidents who currently rely too much on centralized corporate services like Facebook and Amazon to store their data and disseminate their media messages. The problem, he explained in a speech, was caused by the creation of a standard service architecture that is "very subject to misuse" because it consists of "vast repositories of hierarchically organized data about people at the edges of the network that they do not control." When the police show up with a warrant at the offices of the company that controls the network, the company must hand over the data. Moglen's idea is to create a network of cheap and small servers, no larger than a cell phone plug that would be locally controlled by individuals, linked together as a decentralized network, so that

citizens' data cannot be acquired by authorities or any other powerful entity from any one centralized place. Such a system would enable people to back up their data, publish, and communicate securely—all anonymously if they so wish.

As of mid-2011 Diaspora and FreedomBox remained in developmental and experimental stages. StatusNet was being used by a number of tech-savvy communities but has so far failed to gain widespread traction as a noncommercial alternative to Twitter. It remains unclear whether large numbers of people will ever be interested in switching from large commercial brand-name services to more secure and locally controlled alternatives.

Wide adoption of noncommercial tools and services is certainly not unheard of, however, if they are user-friendly enough and offer clear value for many people. Nonprofit organizations, individual activists, independent media organizations, and low-budget educational institutions all over the world rely on WordPress, the open-source blogging platform, and Drupal, the open-source content management system, both of which are developed, maintained, and upgraded by a community of volunteer developers. Another extremely successful project dedicated to developing open-source software that helps ordinary nontechie Internet users gain greater control over their online lives is Mozilla. Its Firefox browser, an open-source volunteer-developed web browser that allows for a high degree of customization, now makes up roughly 30 percent of the world's web browser usage. Firefox integrates the work of other developers through add-ons and plugins, including many that help increase people's privacy and security online. One of these is the Torbutton, integrated with Tor, which enables users to surf the web anonymously and circumvent blocked websites. The Mozilla community also works on a range of other software tools, including the open-source e-mail client Thunderbird, which has become the preferred e-mail client for many activists because it is easy to encrypt, in addition to being free.

Even though a handful of the projects listed above (particularly Commotion Wireless and many but not all of the circumvention tools) do

receive some government and corporate support, many of the programmers and engineers involved in building the global technical commons are part of a hacker counterculture that distrusts all authority and all institutions. This culture is epitomized by groups like the Chaos Computer Club (CCC), which became famous soon after it was founded in Berlin in 1981 after some of its members hacked into the German post office's computer network to expose the network's inadequate security measures. Once every four years the group holds an event called the Chaos Communication Camp in an open field. Generators are set up to power an ad hoc wireless network; workshops are held in tents. The 2011 schedule included topics like "Running Your Own Services to Improve Privacy"; "How to Set Up Your Own Not-for-Profit ISP"; "Blackout Resilient Technologies"; and "How to Bypass the New Data Retention Law." These extraordinary summer hack-fests are complemented by yearly winter conferences the CCC website describes as a "diverse audience of thousands of hackers, scientists, artists, and utopians from all around the world." It is at such events that many of the new tools and techniques of digital resistance are first tested and deployed.

UTOPIANISM VERSUS REALITY

In 1996, John Perry Barlow famously wrote a manifesto titled "A Declaration of the Independence of Cyberspace." It began, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather." In the sixteen years since, government has certainly not left "us" alone in cyberspace—not in small part because many of "us" sought government help in defending us from the criminals, pedophiles, bullies, industrial spies, racists, terrorists, and others who have extended their activities into cyberspace. Meanwhile, corporations have built their own private sovereignties that sometimes challenge—and sometimes collude with—government sovereignties.

Some activist programmers and intellectuals now believe the solution to the twin ills of government interference and unaccountable corporate conduct is to abandon the government- and corporate-addled Internet and build a new one—or a new extension of it—that can be independent of both. In a widely quoted January 2011 essay, media theorist Douglas Rushkoff called on the netizens of the world to unite: "Instead of pretending that the Internet was ever destined to be our social and intellectual commons," he wrote, "we can much more easily conspire together to build a real networked commons, intentionally. And with this priority embedded into its very architecture and functioning." Realizing such an ideal, however, is problematic on both practical and ideological levels.

On a practical level, activists cannot wait for the ideal world to be built. The point of activism is to reach, convince, and engage the largest number of people as quickly and effectively as possible. As Clay Shirky has pointed out, technology becomes most powerful only after it has become commonplace. "The invention of a tool doesn't create change," he writes in *Here Comes Everybody*. "It has to have been around long enough that most of society is using it." Ethan Zuckerman's "cute-cat theory of digital activism" makes a similar point, based on his own experience over years running both commercial and nonprofit platforms. He observes that online activism is most effective when it is carried out through platforms and services that were created not for earnest and civic purposes, but rather for frivolity and fun: online spaces that most people use to socialize, follow and discuss sports teams and movie stars, show off pictures of their babies, and—naturally—trade silly photos of each other's cats. The most popular destinations for online fun and frivolity are of course commercially operated.

Creating noncommercial digital spaces tailor-made for activism has other challenges, as the group WITNESS discovered firsthand. Launched in 1992, WITNESS is a Brooklyn-based nonprofit organization whose primary mission is to help organizations use video to document human rights abuses and advance human rights causes. For the first decade of the organization's existence, it focused mainly on training

activists in video shooting and editing, and in serving as a bridge between activist groups and the global media. By 2005, with the launch of YouTube and other video-sharing sites, it was clear that commercial video-sharing platforms were a powerful tool for activists. But there was a problem: commercial platforms failed to address human rights activists' need for safety, security, and privacy.

As an answer to this problem, in 2007 WITNESS launched its own Video Hub—a sort of YouTube for human rights activists, if you will, tailored to activists' concern for privacy and security, among other needs. They ran the Video Hub for two years before deciding to close it down. One reason was that the technical challenge and expense of hosting vast amounts of video, as well as keeping the site user-friendly and defending it from attack, became insurmountable for a nonprofit organization. The second reason had to do with audience. "Very practically," wrote WITNESS Director Yvette Alberdingk Thijm, "this means that we will more proactively go where people are, as opposed to asking them to come to us."

WITNESS shifted to a new model of curating video posted by activists on other video-sharing websites, most of them commercially operated. That did not, however, stop them from trying to address the problem that inspired them to start the Video Hub in the first place: commercial platforms continue to fail regularly in addressing activists' needs, risks, and concerns. WITNESS has worked directly with YouTube to help its staff develop better, more activist-friendly policies and procedures to minimize the chances that activists' videos would not get removed due to misunderstandings by company "abuse" teams about the nature of their video as well as misunderstandings on the activists' part about the company's terms of service. In 2010 the organization collaborated with YouTube on a guide to "Protecting Yourself, Your Subjects, and Your Human Rights Videos on YouTube." YouTube sent a senior executive to the 2010 Global Voices Citizen Media Summit in Santiago, Chile—a gathering of bloggers from all over the world—to explain its system and learn more about digital activists' concerns.

At various times, members of the Global Voices community have discussed whether it would make sense to develop a blog-hosting or social media platform for online activists, given all of the problems activists have faced with commercial platforms. In the end, however, Global Voices decided that this was no more likely to succeed than WITNESS had been, for the same reasons. Global Voices uses a combination of open-source tools, noncommercial platforms, and commercially operated services. This further reinforces how important it is that the citizen commons—given its symbiotic relationship with the commercial sector—must engage and push companies to behave in a manner that is not only profitable for the long term but also serves the greater public good.

Cyber-separatism has ideological dangers as well. Attempts have been made over the past century to build government- and corporate-free communities in the physical world. Most have turned out disappointingly for most of the participants, who eventually returned to more conventional lifestyles, failed to become economically sustainable, developed their own governance problems that led to bitter conflict, or all of the above. The hippie communes of the 1960s were less comfortable and harmonious in reality than in theory. Earlier in the twentieth century, revolutionary attempts to create capitalism-free societies in the former Soviet Union, Eastern Europe, China, and elsewhere were rather disastrous when it came to human rights, let alone economic prosperity. Utopian ideologies such as Marxism-Leninism and Maoism produced demagoguery, totalitarianism, and genocide.

In a controversial 2006 essay about what he calls "Digital Maoism," and later in his 2010 book, *You Are Not a Gadget*, technologist Jaron Lanier warned of a "new online collectivism," the digital variant of a concept that "has had dreadful consequences when thrust upon us from the extreme Right or the extreme Left in various historical periods." Though there is much idealism and enthusiasm around the idea of the Internet being a place where the evils, hypocrisies, and general messiness of human economics, politics, and social relations can somehow be transcended, there is little evidence that human nature is any more virtuous or selfless in cyberspace than it is in the physical world. Yet there is copious evidence that the Internet can amplify and telescope both the

good and the evil aspects of human nature. Movements to create an ideal society through the creation of online communities led by charismatic leaders with utopian visions claiming to transcend all of the political ambiguities and hypocrisies of "meat space" are more than likely to produce Internet-age versions of the same problems that caused tremendous human suffering in the twentieth century.

A related danger is technological determinism: the belief that technology can be used to solve problems whose roots ultimately lie in human social and ethical behavior. Placing excessive expectations on the ability of technology to defeat repression can cause individuals to abdicate individual responsibility. Variants of technological determinism are often spouted by Internet company executives, who claim that by making the world more connected, they are inevitably and inexorably helping to make it more democratic in the long run, whatever the short-term compromises or collateral damage might be. This argument is wearing thin against attempts such as the Global Network Initiative to convince companies that they need to allow themselves to be held publicly accountable if they want the public to trust them over the long term.

Technological determinism is as dangerous as historical determinism, the worldview underpinning the philosophies of Marx and Hegel, who believed that history was inevitably and inexorably moving the human race toward a certain endpoint. Marxist revolutionaries believed they were in the vanguard of the historically inevitable. Karl Popper, in Volume Two of *The Open Society and Its Enemies*, his seminal 1945 defense of liberal democracy, warned that historicism "is in conflict with any religion that teaches the importance of conscience." Real human progress, he argued, can be achieved only "by defending and strengthening those democratic institutions upon which freedom, and with it progress, depends. And we shall do it much better as we become more fully aware of the fact that progress rests with us, with our watchfulness, with our efforts, with the clarity of our conception of our ends, and with the realism of their choice."

Certainly we can and should use technology to do precisely that. Just because revolutionary cyber-Soviets or Robin Hood–style cybervigilantism are not the answers to our problems does not mean that business and government as we know them today are serving the needs of today's citizens and netizens. New approaches to governance, accountability, and politics clearly are needed if democracy is to survive and thrive in the Internet age.

GETTING POLITICAL

It is not realistic for most people living in developed Western countries to live independently from corporate products and services. It is similarly unrealistic for all but the most dedicated and technically adept people to live their digital lives independent of corporate services. This is why political activism to push for netizen-centric corporate practices and government policies is essential. Companies did not adopt responsible environmental and labor practices of their own accord: they grew more responsible and accountable with their environmental and labor practices as a result of many decades of activism, investigative journalism, public pressure, and debate. If it had not been for decades of such activism, governments would not have moved forward in these areas either.

Similarly, ensuring that the Internet serves netizens' aspirations for democracy and accountable governance—and is not used ultimately to quash and manipulate these aspirations—is going to require a robust and diverse ecosystem of efforts and organizations over many years. The Internet freedom movement has not even arrived at the same point of global public awareness that the environmental movement achieved by the first Earth Day in 1970. There is much work to do.

Within the global environmental movement, some organizations and initiatives have seen value in working with corporations and governments. Others are opposed to compromise and insist on radical alternatives as the only course. All points on the spectrum need to exist for progress to be made. Meanwhile, in universities, students are starting to create activist organizations. The experience with student-driven movements for South African divestment in the 1970s and '80s, Sudan divestment activism in the mid-2000s, and on-campus chapters of

Amnesty International, Greenpeace, the Sierra Club, and others shows just what a critical and catalytic role students can play in promoting change when they get organized. One new organization, devoted to promoting and building the digital commons, is Students for Free Culture. Perhaps it is time for some talented and passionate young people to take the lead in launching a new global alliance: Students for Internet Freedom, anyone?

Just as green parties have emerged over the past several decades from the environmental movement, and labor parties emerged from the labor rights movement of an earlier generation, a new generation has begun to organize political parties and focus political platforms with a strong focus on Internet rights. Branches of the provocatively named Pirate Party now exist in at least twenty-five countries and have gotten candidates elected to local office in Spain, Switzerland, Germany, and the Czech Republic. In 2009 Sweden's Pirate Party won two seats in the European Parliament with 7 percent of the Swedish vote thanks mainly to the support of people under thirty years old. When Amazon's web-hosting service dropped WikiLeaks as a customer, the Swedish Pirate Party welcomed WikiLeaks to its secure and surveillance-free ISP, launched in mid-2011 in defiance of Sweden's data-retention laws. The Pirate Party has its origins in battles over copyright law and enforcement, and in defending citizens' right to use file-sharing websites. However, the party's recent electoral success at least in Sweden is due to a broadening of its platform to the fight against censorship and surveillance, which appeals to a much wider range of voters. In other European countries, green parties have taken up Internet freedom as a signature issue alongside environmental and social justice concerns.

Still, much of the public discourse about censorship and surveillance is found mainly in online niche media, blogs, and social media networks, read by niche communities of tech-savvy young people. Unlike environmental and labor issues, about which there is broad global awareness, there is much less so of the threats to Internet freedom and how these threats cut across regions, ideologies, systems of government, and

corporate platforms. Major news organizations generally treat Internet-related news as a business, consumer, or cultural subject; with a few notable exceptions, the Internet generally is not covered as a politically contested space in which citizens need to engage to ensure their rights are upheld. Rather than wait for this to change, people and organizations with expertise and experience to share can report directly through blogs and independent websites, and in this way influence public debates as well as the broader news agenda.

To this end, universities and research institutes are starting to build research programs across disciplines—from computer science and political science to business, economics, and sociology—that help policy makers, companies, and citizens better understand the threats to Internet freedom around the world and how they can be counteracted. Teams at Harvard's Berkman Center, the University of Toronto's Munk Centre, the Oxford Internet Institute, Princeton's Center for Information and Technology Policy, and many others have contributed much of what the world knows—and what the media reports—about global Internet censorship and surveillance, cyber-attacks against digital activists, corporate practices that both extend and diminish freedom, and how different laws can either protect or erode civil rights in the digital environment.

A growing number of nongovernmental organizations are also dedicating themselves to Internet policy advocacy: informing the public about complicated issues that the news media often doesn't cover well, and lobbying governments to change or improve laws so the Internet can remain as open and free as possible. The Electronic Frontier Foundation and the Center for Democracy and Technology are just two of many such groups in the United States. Counterparts exist all over the world: the Open Rights Group in the UK, Bits of Freedom in the Netherlands, Netzpolitik in Germany, La Quadrature du Net in France, Jinbonet in South Korea, and many others. Other more globally focused organizations such as the South Africa–based Association for Progressive Communications are working to coordinate policy strategy on a global level, lobbying the United Nations Human Rights Council, the

Internet Governance Forum, ICANN, the OECD, and other regional and international organizations.

Ad hoc coalitions of these groups are also working to involve more netizens from around the world in global Internet governance debates and processes. In an effort to build consensus around the common values that netizens' groups are fighting for, the Dynamic Coalition on Internet Rights and Principles—a multi-stakeholder group composed mainly of activists and academics from around the world who have been meeting annually at the Internet Governance Forum and working throughout the year mostly through e-mail and Skype—spent two years collectively drafting a Charter of Human Rights and Principles for the Internet. Their aim is not to invent new rights, but to take rights that have long been considered universal in the physical world and translate them into the digital context. In early 2011 in conjunction with the Internet freedom advocacy group Access Now, they published a summary of the charter's ten core principles:

1) *Universality and Equality*
   All humans are born free and equal in dignity and rights, which must be respected, protected, and fulfilled in the online environment.
2) *Rights and Social Justice*
   The Internet is a space for the promotion, protection, and fulfilment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.
3) *Accessibility*
   Everyone has an equal right to access and use a secure and open Internet.
4) *Expression and Association*
   Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural, or other purposes.

5) *Privacy and Data Protection*
   Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal, and disclosure.
6) *Life, Liberty, and Security*
   The rights to life, liberty, and security must be respected, protected, and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.
7) *Diversity*
   Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.
8) *Network Equality*
   Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritisation, filtering, or traffic control on commercial, political, or other grounds.
9) *Standards and Regulation*
   The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion, and equal opportunity for all.
10) *Governance*
    Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation, and accountability.

Many of these principles go far beyond what Western democratic governments are prepared to support. Some clash dramatically with the positions of many of the world's most powerful Internet and

telecommunications companies. Even so, the process of formulating these principles demonstrates that when the Internet's future is viewed through a human rights and social justice lens instead of a commercial or national security lens, major disagreements can emerge even when governments and companies agree in principle on the need for an open, globally interconnected Internet as well as protection and respect for human rights and free speech.

In June 2011 the Paris-based Organisation for Economic Co-operation and Development (OECD) published a "Communiqué on Principles for Internet Policymaking," signed by forty governments and two nongovernmental stakeholder groups: one representing business and industry and the other representing the Internet technical community. The document was heralded by the United States and other governments as an important foreign policy consensus, at least among the world's major democracies, on core principles for safeguarding the open Internet and free flow of information, as well as the need for balance between the need to protect civil liberties and governments' need to provide security and protect business. Yet a third group that also participated in negotiations over the text of the communiqué—the civil society constituency whose members included groups advocating for free expression, privacy, and consumer rights—could not endorse the document.

Though the civil society members welcomed the communiqué's commitment to human rights, rule of law, and freedom of expression, they were unable to support it for two main reasons. The document, they said in their dissenting statement, placed excessive emphasis on cyber-security and intellectual property enforcement in a manner that could potentially be used to justify policy trade-offs that human rights groups believe to be unacceptable. An even greater concern was vague language calling for Internet intermediaries such as ISPs and social networking platforms to take on more responsibility in policing their services. They warned that Internet intermediaries "are neither competent nor appropriate parties" to make decisions about the legality of content posted or transmitted by their users. "Requiring them to make determinations on the legality of content or behaviour of users raises issues for transparency, due process and accountability and detrimentally impacts on citizens' freedom of expression."

It is unlikely that the OECD Internet principles would have been heralded as a step in the right direction if either the business or the technical community had refused to sign on. Despite the lack of support from groups concerned with human rights, free expression, and social justice, members of the Obama administration involved with Internet policy praised the principles as a way forward for governments to "address policy challenges" without violating fundamental rights. The document laudably helps to build a consensus among democracies around a shared commitment to open, globally interoperable Internet standards and the free flow of information—in stark contrast to the Internet governance policies of China and other authoritarian nations. At the same time, it shows that democratic governments remain in denial about an insidious reality at the digital intersection of governmental and corporate power: power over citizens' digital lives is being exercised in increasingly opaque and unaccountable ways.

Elected democratic governments are likely to remain in denial unless and until their electorates give them meaningful political incentives—both positive and negative—to change their priorities. Over time, the environmental, labor, and traditional human rights movements built powerful political constituencies that have shifted the domestic and international policy priorities of most of the world's democracies. There is no reason an Internet freedom movement cannot eventually do the same thing, with enough effort by enough people.

CORPORATE TRANSPARENCY AND NETIZEN ENGAGEMENT

The power of corporations to shape netizens' digital discourse and hence our political lives will not be constrained without new mechanisms and strategies for collective bargaining by netizens with corporations. The existing political and legislative processes of nation-states are failing to

do the job. While it makes no sense for a company to try to duplicate the mechanisms of representative parliamentary democracy within their global constituencies, the status quo is also unacceptable. Netizens, companies, and governments all face an urgent moral imperative to innovate politically—in the broadest sense of the word—on a scale that matches the dramatic technical innovations of the past several decades.

Aside from the Global Network Initiative's nascent attempt to create a system of accountability for Internet and telecommunications companies, a few even more embryonic efforts to push companies in a more netizen-centric direction have begun to take shape. They will all require much broader global participation and awareness to be effective:

Boosting corporate transparency. This is essential to prevent the abuse of citizens' rights—be it by governments or by companies. As citizens, we have a right to know how our information is shared, with whom, and under what circumstances. We also have a right to know how our access to information, as well as our ability to disseminate it, is being shaped by any given service or platform. At the moment, this right is respected by few companies or governments.

Companies should be required to report regularly and systematically to the public on how content is policed, and under what circumstances it gets removed or blocked and at whose behest. In the summer of 2010, motivated by its commitments as a member of the Global Network Initiative, Google took a step in this direction by launching a website called the Transparency Report, tracking the numbers of requests it receives from governments to take down content or hand over user information, broken down by country. (Ironically, China had to be excluded because of Chinese state secret laws that could endanger local Google employees if the data were released.) With the caveat that requests from China prior to Google's withdrawal of its search engine are a black hole, the greatest volume of known requests in July through December 2010 came from democratically elected governments, with the US government well in the lead, followed by Brazil, India, and the United Kingdom.

Though the data are not complete and there are many unanswered questions, Senior Counsel Nicole Wong explained in a speech soon after the report's 2010 launch that Google's intent was to use data "as a basis to start a conversation about censorship and surveillance." She pointed out that "we see requests in almost every country in almost every election period." Another section of the Transparency Report tracks the accessibility of all of Google's services country by country, in close to real time. This tool enables people around the world to see which countries are deliberately blocking YouTube, Gmail, Blogspot, or any other Google services, as well as when traffic is cut off altogether. (Statistics quickly dropped to zero during the Egyptian blackout, for instance.) Governments should support this effort if they consider themselves in the least bit democratic.

Google has also invested in transparency tracking that goes beyond its own services. It has partnered with the New America Foundation's Open Technology Initiative on a project called the Measurement Lab, or M-Lab, an open platform that seeks to build tools and collect data that will help Internet users compare and evaluate the quality of broadband connections around the world. The tools include a "glasnost test," which can be used to check whether a given broadband connection is blocking or throttling performance of certain applications. A "mobile traffic test" enables users to determine whether a mobile Internet provider is discriminating between applications or services. Of course, it would be ideal if all mobile and broadband service providers around the world were more transparent with users about such information from the beginning. The hope is that projects like the M-Lab will push other companies in the same direction.

Netizens should demand that Internet and telecommunications companies follow Google's lead and improve upon it. All companies must publicly and clearly show how they gather and retain our information; how they share that information both with government and other companies; and in what way they may be shaping or prioritizing certain types of data over others. In doing so they can credibly demonstrate to us, as their constituents, that they recognize and take seriously

the power they hold over us in the quasi-public spaces they operate, and they understand their duty to wield that power responsibly.

Building a more citizen-centric and citizen-driven information environment. As marketing guru and consumer advocate Doc Searls likes to say: "We have a submissive relationship with services." Internet and telecommunications services and platforms dictate the terms. We have no role in the conception or formulation of the terms; we are merely offered the choice of clicking "agree" or not.

"Individuals need to be at the centers of their own digital lives, and not peripheral dependents either of vendors or identity providers," Searls explains in the tenth-anniversary edition of a seminal book that he coauthored, *The Cluetrain Manifesto*, about how the Internet has turned markets into conversations. Searls and a group of software developers, businesspeople, and consumer advocates are working on a set of projects described as Vendor Relationship Management, or VRM. The aim is to empower netizens in shaping the terms of our relationships with companies. Specifically, the goals include:

1. Provide tools for individuals to manage relationships with organizations.
2. Make individuals the collection centers for their own data, so that transaction histories, health records, membership details, service contracts, and other forms of personal data aren't scattered throughout a forest of silos.
3. Give individuals the ability to share data selectively, without disclosing more personal information than the individual allows.
4. Give individuals the ability to control how their data is used by others, and for how long. This will include agreements requiring others to delete the individual's data when the relationship ends.
5. Give individuals the ability to assert their own terms of service, reducing or eliminating the need for organization-written terms of service that nobody reads and everybody has to "accept" anyway.

For such a world to be realized, companies and governments must actively support its development. As netizens we should demand that they do so.

Creating a more netizen-centric and netizen-driven information environment even holds lucrative opportunities for forward-thinking entrepreneurs and businesses. In January 2011 a report by the World Economic Forum declared personal data to be a new "asset class" and a "post-industrial" business opportunity for "a host of new services and applications" that can increase "the control that individuals have over the manner in which their personal data is collected, managed and shared." This insight is a classic example of what the *Harvard Business Review*'s Kramer and Porter called "shared value": the identification by forward-thinking entrepreneurs of business opportunities whose very purpose is to empower people.

Building processes for corporate engagement with users, customers, and other stakeholders. Anger over identity policy on Facebook and Google Plus, problems caused by Facebook's privacy policy changes, the disastrous Google Buzz rollout, and Flickr's clashes with activists might all have been prevented if companies adopted more innovative ways to engage with netizens around the world who are affected by their businesses. A way must be found for companies to work more directly with netizens, their constituents, in shaping products and services. Netizens need to devise more systematic and effective strategies for organizing, lobbying, and collective bargaining with the companies whose services we depend upon—to minimize the chances that terms of service, design choices, technical decisions, or market entry strategies could put people at risk or result in infringement of their rights.

The idea that companies can and should engage with user and customer communities is not new. In his book *Democratizing Innovation*, MIT professor Eric von Hippel documents an important trend in innovation: many of the world's most dynamic and innovative companies now involve customers and users directly in developing new products

or improving on existing ones. Von Hippel found this to be the case in a range of industries, including medical devices, computer hardware and software, and a range of consumer products. It is now time for Internet and telecommunications companies to innovate politically, in the broadest sense of the word: build processes for engagement with users and customers, who are re-envisioned as constituents. Invent tools for bottom-up, constituent-driven innovation when it comes not only to developing profitable features, but also to anticipating threats to people's rights and civil liberties. Involve us directly in figuring out how best to mitigate those threats.

PERSONAL RESPONSIBILITY

Ai Weiwei, the outspoken artist who helped design the Beijing Olympic stadium before becoming a full-time thorn in the government's side, disappeared from the Beijing airport on April 3, 2011, as he prepared to board a flight to Hong Kong. For more than a month, nobody knew where he was. A month later, his wife was allowed to visit him in detention. A vague news report claimed he was facing charges of tax evasion, although the tax bureau, when contacted by journalists about the case, claimed to have no information. In mid-June 2011 he was finally released.

After the devastating 2008 earthquake in Sichuan province, Ai used his fame and influence to support and promote efforts by local families, activist bloggers, and human rights lawyers to compile and disseminate information about the children who had died in schools that collapsed while surrounding buildings remained intact. Corrupt local officials had allowed construction firms to cut corners on school buildings across the province. Angry parents wanted answers. They wanted those responsible to be punished. Instead the government detained several activists and convicted a few on charges of subversion. Names of people and places related to this accountability movement, as well as a range of related phrases, were put on the list of things that Internet companies must remove from blogs and social networking sites. Ai Weiwei's name, and all discussion of his case, is also banned from China's social networking platforms.

If Facebook—or any other global social network—were to set up shop in China, authorities will expect company employees to block Ai Weiwei fan pages and to erase pages created by families in Sichuan to raise awareness about what happened to their children. Police will expect the company to hand over all personally identifying information about the Chinese users who create such pages, and suspend their accounts. If activist programmers try to create iPhone apps through which people can report corruption, or a "Free Ai Weiwei" app featuring pictures of his art, they can count on being censored by Apple's Chinese app store. Such is the price of doing business in China. Similar prices are demanded with increasing frequency by governments around the world.

The first time I visited Ai Weiwei at his home was on a frosty Beijing morning in January 2009. He was just having breakfast. We sat at his kitchen table as he ate a bowl of rice porridge and a couple of meat-filled steamed buns, and talked about personal responsibility. "Either you're part of the crime, or you're compassionate," he said. "We will never have a real civil society, a democratic society, unless people take responsibility." He took a bite of steamed bun and washed it down with porridge, then continued:

> Why do I want to take any responsibility? Democracy is not a political ideal. Democracy is a means of handling problems. This method is effective—why? Because everybody in society takes responsibility. If nobody is taking responsibility, it shouldn't be called "society." Or it's a slave society anyway. . . .
>
> Even people in the police, even people who make policy, they are all able to make choices. Otherwise my blog wouldn't survive. There are always people who insist. One person says, "This post has to be deleted," but another says, "It's best not to delete it." I believe somebody must have worked to make it happen. So I believe the desire for justice and equality is something that people must have in their own hearts. This isn't something that one

person can give to another. This is a right that must be exercised. If you don't exercise your right, society will be in a difficult state.

Later that year Ai's accounts on two different Chinese blog-hosting platforms were deactivated.

It will take time—and much work and sacrifice by a great many people—to figure out how to bring "consent of the networked" to life in a messy, complicated, and rapidly evolving world. The way forward will most certainly involve a great deal of trial and error. Conflict and abuse of power will never disappear from any human society. But as Ai points out, every person has the ability to influence the political future depending on who and where we are.

Whether we are simply users of technology, investors in technology companies, employees or executives of Internet-related companies, elected officials, or mid-ranking government bureaucrats, we all have a responsibility to do whatever we can to prevent abuse of digital power, and avoid abusing it ourselves. We have a responsibility to hold the abusers of digital power to account, along with their facilitators and collaborators. If we do not, when we wake up one morning to discover that our freedoms have eroded beyond recognition, we will have only ourselves to blame.

http://consentofthenetworked.com

NOTES

CHAPTER 1: CONSENT AND SOVEREIGNTY

5 **"Before things were simple: you had the good guys on one side, and the bad guys on the other. Today, things are more subtle":** Jailan Zayan, "Egypt, Tunisia Finding that Road to Freedom Is Rocky," Agence France Presse, May 26, 2011.

6 **President Barack Obama waxed enthusiastic about the political power of social networking:** Full transcript at www.whitehouse.gov/the-press-office/2011/04/20/remarks-president-facebook-town-hall (accessed June 21, 2011).

7 **A classic example was Google's clash with the Chinese government:** A full account of those events can be found in Steven Levy, *In the Plex: How Google Thinks, Works, and Shapes Our Lives* (New York: Simon & Schuster, 2011). Also see John Pomfret, "In China, Google Users Worry They May Lose an Engine of Progress," *Washington Post*, March 20, 2010, www.washingtonpost.com/wp-dyn/content/article/2010/03/19/AR2010031900986.html (accessed June 21, 2011).

9 **geopolitical vision for a digitally networked world:** Eric Schmidt and Jared Cohen, "The Digital Disruption: Connectivity and the Diffusion of Power," *Foreign Affairs* 89, no. 6 (November/December 2010), 75–85.

10 **In his book *The Filter Bubble*, Eli Pariser:** Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (New York: Penguin Press, 2011).

10 **Siva Vaidhyanathan warns:** Siva Vaidhyanathan, *The Googlization of Everything (And Why We Should Worry)* (Berkeley: University of California Press, 2011).

10 **As Harvard's Joseph Nye points out in *The Future of Power*:** Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011).

11 **Other kinds of transnational organizations are also challenging the power of nation-states:** One of the earliest policy analyses of the challenge posed by transnational organizations to the power of nation-states, and how the Internet had amplified the power of new actors, was by Jessica T. Matthews, "Power Shift," *Foreign Affairs* 76, no. 1 (January/February 1997), 50–66. Parag Khanna argues that the world is entering a new phase that he calls the